DETERMINING A CAUSE OF A REDUCED PERFORMANCE OF SERVICE IN A COMMUNICATIONS NETWORK

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application is the US National Stage of International Application No. PCT/DE2003/002278, filed July 8, 2003 and claims the benefit thereof. The International Application claims the benefits of German application No. 10231149.8 filed July 10, 2002, both applications are incorporated by reference herein in their entirety.

FIELD OF THE INVENTION

[0002] The present invention relates to a method for detecting a cause of a reduced performance of service in a communications network, as well as a system for controlling and monitoring a communications network, and a control program for a device to monitor service quality and/or faults.

BACKGROUND OF THE INVENTION

[0003] Network operators in the telecommunications market offer numerous services to customers, particularly Internet services. The services which network operators offer are divided into different service quality levels, in order to satisfy customer requirements according to guaranteed service levels and to stand out from competitors. For example low-cost services are on offer for private customers, and services with enhanced features are on offer at higher cost for business customers. Such enhanced service features may for instance include guaranteeing a high level of availability and low data loss. For this purpose network operators and their customers enter into service level agreements (SLA) defining the scope and quality of services to be provided to customers. Particular significance is then attached to proving that the service level agreement with a given customer has been maintained. Providing such proof requires services to be monitored, for example in order to record faults and determine the availability of a service. Measurements are also carried out in order to record service quality parameters such as data loss. The provision of services is therefore not simply confined to the administration of service parameters such as the bandwidth or call number, but also includes controlling

additional, service-specific functions.

[0004] To ensure that the effects of failing to maintain a service level agreement are kept to a minimum for both the network operator and the customer, reliable and rapid detection of reduced service performance is indispensable.

SUMMARY OF THE INVENTION

[0005] The object of the present invention is to create an efficient and reliable method for detecting a cause of a reduced performance of service, as well as to specify a suitable implementation of the method, along with a communications network control and monitoring system suitable for carrying out the method.

[0006] This object is achieved by the claims. Advantageous embodiments of the method according to the invention are specified in the dependent Claims.

[0007] Inventively, an essential precondition for efficiently and reliably detecting a cause of a reduced performance of service consists in first of all testing selected services for service quality and/or availability to determine any services which are affected by a reduced service performance. The test of service quality and/or availability can be adapted to requirements placed by users of a communications network on the services they use. By this means test results are as far as possible representative of the service quality and/or availability perceived by the users. As soon as the services affected by a reduced service performance are determined, network elements which are relevant to the provision of these services according to information stored in a network element database can be tested selectively to determine responsibility. This offers the advantage that it is unnecessary to subject largely similar network elements to continuous testing in order to form opinions concerning services which are potentially faulty or at risk. The effect of the present invention is therefore to significantly reduce the total cost of monitoring network elements

reliably.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is explained in greater detail as an exemplary embodiment with reference to the drawings, in which:

Figure 1 shows a schematic representation of a communications network control and monitoring system,

Figure 2 shows a flow chart of a method for determining a cause of a reduced performance of service in a communications network.

DETAILED DESCRIPTION OF THE INVENTION

[0008] The diagram of a communications network control and monitoring system shown in Figure 1 comprises a service provision device 101, a communication connection management device 102, a fault-monitoring device 104 and a service quality monitoring device 105.

[0009] The service provision device 101 is intended for arranging or changing services. For this purpose the service provision device 101 receives messages 121 with service requests and converts these into messages 122 with connection requests which are transmitted to the communication connection management device 102.

[0010] The communication connection management device 102 is intended for storing information that describes network elements, which are relevant to the provision of a service, with regard to their functional properties and their topological arrangement. This information is assigned to the appropriate service and stored in a network element database 103 associated with the communication connection management device 102. The network elements that are relevant to the provision of a service include such items as network access points, ports and line connections along an end-to-end network path between two service access points. Functional properties of network elements include bandwidth, the supported communications protocols and the switching technologies used. The

description of the topological arrangement of network elements comprises sub-dividing the network elements into node network elements such as measurement points and switching points, and branch network elements such as line connections, in the form of topological information prepared according to a node-branch model. The information stored in the network element database 103 can be retrieved by the fault-monitoring device 104 and the service quality monitoring device 105.

[0011] When a service is being arranged or changed, the service provision device 101 sends the fault-monitoring device 104 a message with a request to monitor the availability of network elements that are specified as relevant to the provision of the service concerned. In the same manner a message 125 with a request to monitor the service quality is transmitted to the service quality monitoring device 105. These monitoring requests cause the fault-monitoring device 104 and the service quality monitoring device 105 to compare fault messages 127 and measured values 128, detected in sub-networks 106, 107, 108, and forwarded to the fault-monitoring device 104 or the service quality monitoring device 105 via a network operating system 109, 110, 111 assigned to the respective sub-network, with the information on illegal deviations stored in the network element database 103. For this purpose corresponding network element database information is queried by the fault-monitoring device 104 and/or the service quality monitoring device 105 and sent to them as messages 126. In the event of an illegal deviation from the information stored in the network element database 103 the fault-monitoring device 104 and/or the service quality monitoring device 105 generate a message 129, 130 about a reduced service performance, specifying the service affected.

[0012] Availability and service quality are monitored in accordance with a service level agreement between a customer and a network operator. Therefore the network element database 103 only stores information on the network elements specified by a service level agreement as relevant to the provision of a service. Furthermore

only fault messages and/or measured values about the network elements specified by a service level agreement as relevant to the provision of the service are detected. For the purpose of monitoring the rules defined in the context of a service level agreement, a message 123 with a request to monitor a service level agreement is transmitted by the service provision device 101 to the fault-monitoring device 104 when a service is being arranged or changed. This means that the detection of fault messages and/or measured values about the network elements specified by a service level agreement as relevant to the provision of a service is initiated when the service concerned is arranged or changed.

[0013] If the evaluation of a measured value 128 in the service quality monitoring device 105 reveals that a network element is being operated outside the permissible operating range, the service quality monitoring device 105 sends an alarm message 129 about an infringement of a service quality criterion to the fault-monitoring device 104 where the message is converted into an alarm message 130 about an infringement of a service level agreement. A fault message 127 is converted in the fault-monitoring device 104 directly into an alarm message about infringement of a service level agreement. The alarm message 130 contains a statement about the service availability and/or service quality and, for the purpose of remedying the reduced service performance, is transmitted via a network operating system 109, 110, 111 assigned to the sub-network 106, 107, 108 in which a fault or an infringement of the service quality criterion is taking place. The appropriate network operating system 109, 110, 111 converts the alarm message 130 into a control command 131 and this, in the form of a message for the purpose of remedying the reduced service performance, is transmitted to a selected control device (not shown) in the respective sub-network 106, 107, 108. For the purpose of remedying the reduced service performance, the network element affected by the action to remedy the reduced service performance is reconfigured by the appropriate network operating system 109, 110, 111 which accesses the

information stored in the network element database 103. This also applies to the configuration of a network element when a service is being arranged, changed or deleted.

[0014] The alarm message 130 about an infringement of a service level agreement is also transmitted to the service provision device 101. There it is processed with customer data and converted into a report 132 about compliance with or infringement of a service level agreement.

[0015] The current view is that it is not realistic to solve every problem that arises in a communications network as quickly as possible in order to guarantee service quality and availability. Due to the plurality of services offered to the customers of network operators on the basis of numerous service level agreements, the starting point for any approach to remedying network problems should always be a customer-centered or service-oriented view of available network resources or elements. This makes it necessary to test service quality and availability as perceived by the customer. Important criteria for such a test are service quality parameters such as data transmission rate, latency and phase variations leading to data loss. For this reason it is helpful to check which network problems have an effect on which services, using this information to prioritize the remedying of network problems, for example by reference to service level agreements. Great significance is also attached to early detection of existing network problems which may quickly cause services to become faulty or place them at risk.

[0016] In order to cope with these requirements, the present invention brings together approaches aimed at monitoring network elements or network resources at the physical level on the one hand, and monitoring service quality and availability at the application level on the other. Approaches aimed at monitoring on the physical level only are very close to their limits, particularly in extended, complex networks, since in such cases a plurality of network elements and network resources have to be monitored. In particular

there is a problem that if a central network resource fails it triggers a plurality of consecutive alarm messages. This means that in such critical situations an enormous quantity of information has to be processed under time-critical conditions. A first approach to handling this problem consists in filtering out secondary alarm messages. Whilst approaches aimed at monitoring purely at the application level offer the advantage of a service-oriented or customer-centered view together with pre-consolidation of information regarding the evaluation of alarm messages, they have the disadvantage that test results cannot be used to form opinions about the causes of failures or problems. According to the invention, both the approaches mentioned are combined by providing information concerning the network and service topology.

[0017] The provision 201 of information concerning the network and service topology is the starting point of the inventive method for determining a cause of a reduced performance of service in a communications network, the sequence of which is explained by means of the flow chart shown in Figure 2. For this purpose network elements which are relevant to the provision of a service are described with regard to their functional properties and their topological arrangement, the associated descriptive information being stored in the network element database 103 and assigned to the appropriate service. This is followed by an arrangement 202 for testing provided services and an arrangement 203 to establish a time plan for testing the selected services with respect to service availability and/or service quality. Establishing the arrangement for the services and time plan is followed at preset times and for the selected services by the testing 204 of service availability and/or service quality. This is followed by an evaluation 205 of test results, said test results being used to determine services which are faulty and/or at risk, and which are either immediately or potentially affected by a reduced service performance. The information concerning the network and service topology stored in the network element database 103 is used to carry out a

determination 206 of the network elements to be tested. The network elements determined as needing to be tested are those network elements which are identified in the network element database 103 as relevant to the provision of the service affected by the reduced service performance. There then follows testing 207 of the network elements determined as above, and lastly evaluation 208 of the test results and determination of the network elements responsible for the reduction in service performance.

[0018] Testing 204 of the selected services with respect to service availability and/or service quality is carried out by means of a comparison with the information stored in the network element database 103. The information stored in the network element database describes permissible operating ranges for the network elements. This information is used for the testing 207 of the network elements determined as above, in order to determine a cause for the reduced service performance.

[0019] The network elements so determined are tested to determine the cause of a reduced service performance by such means as detecting status or fault messages for the network elements concerned. These messages can be monitored by the fault-monitoring device 104 or the service quality monitoring device 105 either actively or passively. Furthermore such monitoring can also apply to data processing devices (not shown in Figure 1) which are connected to the communications network shown in Figure 1, as well as to operating system programs or application programs running on these data processing devices.

[0020] For the purpose of testing service availability and/or service quality, the fault-monitoring device 104 and/or the service quality monitoring device 105 provide control sequences containing preset service access requests to be executed on or by selected service access points in the sub-networks 106, 107, 108. This means that a virtual user is set up at the service access point concerned, and this user's behavior is mapped by the service access requests

contained in the control sequence. Such a virtual user can be perceived both as a message source and as a message sink. Since a virtual user is in the main fully controllable by the fault-monitoring device 104 or the service quality monitoring device 105, it can in principle be located on any service access point, for example near the service access points of real users or on interfaces between sub-networks. The control sequences containing the preset service access requests can for example emulate the following scenarios:

- "Internet access" - querying one or more reference Internet pages,
- "E-mail" - sending a reference e-mail to an e-mail server and querying the e-mail from the e-mail server,
- "File transfer" - querying a reference file from a file server,
- "Domain name access" - resolving logical Internet addresses into physical Internet addresses,
- "TCP (transmission control protocol) " - establishing a TCP connection,
- "DHCP (dynamic host configuration protocol)" - querying an Internet address,
- "UDP (user datagram protocol)" - sending a UDF data packet from a data source to a data sink.

[0021] Moreover network elements that are essential to the provision of a selected service can be tested at preset times for their ability to operate, without the service first having to be tested with respect to service quality and/or service availability. This offers the advantage that particularly critical network resources, even those without break points for reduced service performance, can be tested directly. Direct testing of the ability to operate can also include terminals for which testing at selected times has been

defined by a service level agreement between a customer and a network operator. Thus testing of network elements or network resources can refer not only to network operators' own network elements or network resources, but also to customers' own terminals.

[0022] The method described above for detecting reduced service performance can also determine faults in network components which from the network operator's point of view do not belong to that operator's network but rather to a third-party network and are not directly controllable from the network operator's point of view.

[0023] The steps to which the method relates, which are carried out in the service provision device 101, the communication connection management device 102, the fault-monitoring device 104 and the service quality monitoring device 105, are implemented in each case by a control program provided for the service provision device 101, the communication connection management device 102, the fault-monitoring device 104 and the service quality monitoring device 105. The respective control program runs on a data processing device assigned to the service provision device 101, the communication connection management device 102, the fault-monitoring device 104 and/or the service quality monitoring device 105. Depending on the application, it is also possible to use a common data processing device on which the said control programs run either separately or as combined control programs.

[0024] The application of the present invention is not confined to the typical embodiment described here.